Distributed via @police http://www.npa.go.jp/cyberpolice/

平成 28 年7月 20 日

Topic

CGI 等を利用するウェブサーバの脆弱性（httpoxy）を標的としたアクセスの観測について

CGI 等を利用するウェブサーバの脆弱性（httpoxy）を標的としていると考えられるアクセスを観測しています。ウェブサーバの管理者等は、影響有無の確認と、適切な対策の実施を推奨します。

1 CGI 等を利用するウェブサーバの脆弱性（httpoxy）について

CGI（Common Gateway Interface）は、標準入出力や環境変数を経由してデータを受け渡しつつ、ウェブサーバプログラムから外部プログラムを実行する仕組みです。

平成 28 年7月 18 日に、この CGI 等を利用しているウェブサーバに存在する脆弱性[i]が明らかとなりました。同脆弱性は、環境変数 HTTP_PROXY に指定された値をプロクシサーバとして利用して、外部向けの HTTP 通信を行うというものです。CGI 等を利用するウェブサーバにおいて、環境変数 HTTP_PROXY には、外部から送信された HTTP リクエストの Proxy ヘッダに指定された値が設定されます。この場合、攻撃者は環境変数 HTTP_PROXY に不正な値を設定することが可能となります。ウェブサーバからの外部向け HTTP 通信が、攻撃者の用意する不正なプロクシサーバに誘導された場合、攻撃者はプロクシサーバを経由する通信を盗み見ることや、通信内容の改ざん等の中間者攻撃が可能となります（図1）。

なお、当該脆弱性は報告者により、「httpoxy」との呼称が付けられています。

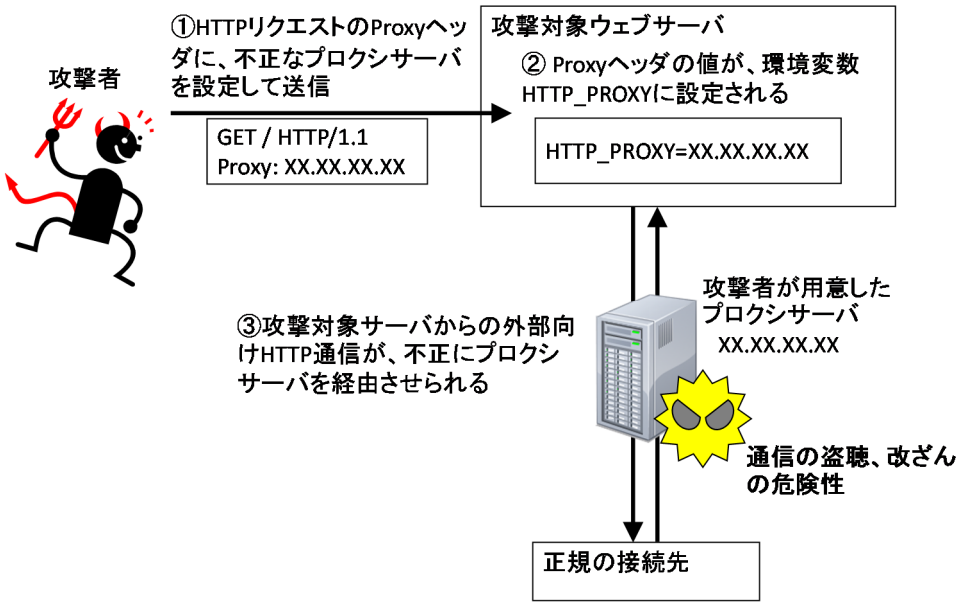

図1 CGI 等を利用するウェブサーバの脆弱性を悪用する攻撃の流れ

[i] https://www.jpcert.or.jp/at/2016/at160031.html
https://jvn.jp/vu/JVNVU91485132/
https://www.kb.cert.org/vuls/id/797896
https://httpoxy.org/

2　CGI 等を利用するウェブサーバの脆弱性（httpoxy）を標的としたアクセスの観測について

警察庁の定点観測システムにおいては、7月 19 日 15 時 41 分以降、当該脆弱性を標的としていると考えられるアクセスを観測しました（図2）。

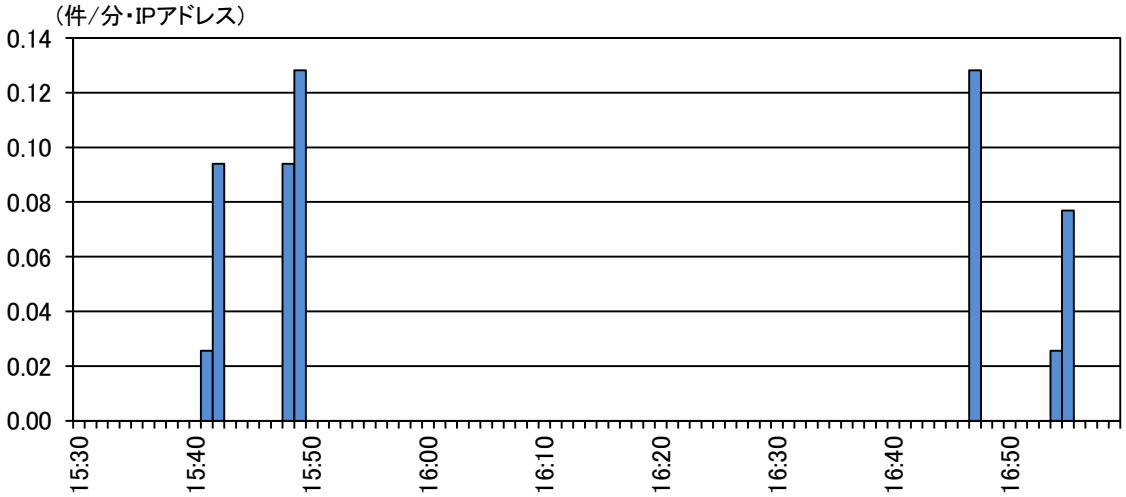

図2　CGI 等を利用するウェブサーバの脆弱性（httpoxy）を標的としたアクセス件数の推移（7月 19 日 15 時 30 分～17 時 00 分）

観測したHTTPリクエストのProxyヘッダには、攻撃者が用意したとサーバのものと思われる IP アドレスとポート番号が指定されていました（図3）。当該 Proxy ヘッダで指定された IP アドレスに対して通信が発生した段階で、攻撃者は発信元となったウェブサーバが当該脆弱性の影響を受ける可能性が高いことが確認できます。また、当該 IP アドレスをプロクシサーバとして経由する HTTP 通信は、攻撃者が通信内容を盗み見たり、改ざんしたりすることが可能となります。

```
GET / HTTP/1.1
User-Agent: masscan/1.0 (https://github.com/robertdavidgraham/masscan)
Accept: */*
Proxy: [redacted]:[redacted]
```

図3　観測した HTTP リクエスト（一部をマスキング）

3 推奨する対策

当該脆弱性は、以下の全ての条件を満たしている場合にのみ、脆弱性を悪用する攻撃を受ける可能性があります。

- 外部からのHTTPリクエストに設定されたProxyヘッダを、制限なく受け入れているウェブサーバである。
- CGI 等を利用しており、HTTP リクエストに指定された Proxy ヘッダの値が、環境変数 HTTP_PROXY に設定される。
- 外部向けの HTTP 通信を行っており、同通信を行うソフトウェアやライブラリに、当該脆弱性が存在する。
- 外部向けの HTTP 通信が制限されておらず、不正なプロクシサーバを経由する HTTP 通信が可能である。

このため、ウェブサーバやウェブアプリケーションの管理者は、影響の有無を確認するとともに、影響を受ける場合には以下の対策を実施することを推奨します。

- 外部からの HTTP リクエストに含まれる Proxy ヘッダを無効にする。
- 当該脆弱性の影響を受けるソフトウェアやライブラリを、脆弱性が修正された最新バージョンにアップデートする。
- 外部向け HTTP 通信を、信頼できる宛先のみに制限する。

当該脆弱性の影響を受けるソフトウェア等は、現時点では以下のとおり判明していますが、その他のソフトウェア等においても、今後当該脆弱性の影響を受ける旨が明らかとなる可能性もあるため、各ソフトウェア等の開発元が公開する情報にも注意してください。

- Apache HTTP Server
- Apache Tomcat Server
- Apache Traffic Server
- Go
- HAProxy
- HHVM
- lighttpd
- Microsoft IIS
- nginx
- Python
- PHP